Electronic Version
Stylesheet Version v1.1.1

[*KEY EXCHANGE BASED ON DSA TYPE CERTIFICATES*]

Abstract

A first certificate is provided from a first peer to a second peer. The first certificate includes a plurality of first parameters. A first exponentiation operation is performed to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer. A second certificate and the first public key from the second peer are provided to the first peer. The second certificate comprises a plurality of second parameters. A second exponentiation operation is performed to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters. A third exponentiation operation is performed to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.